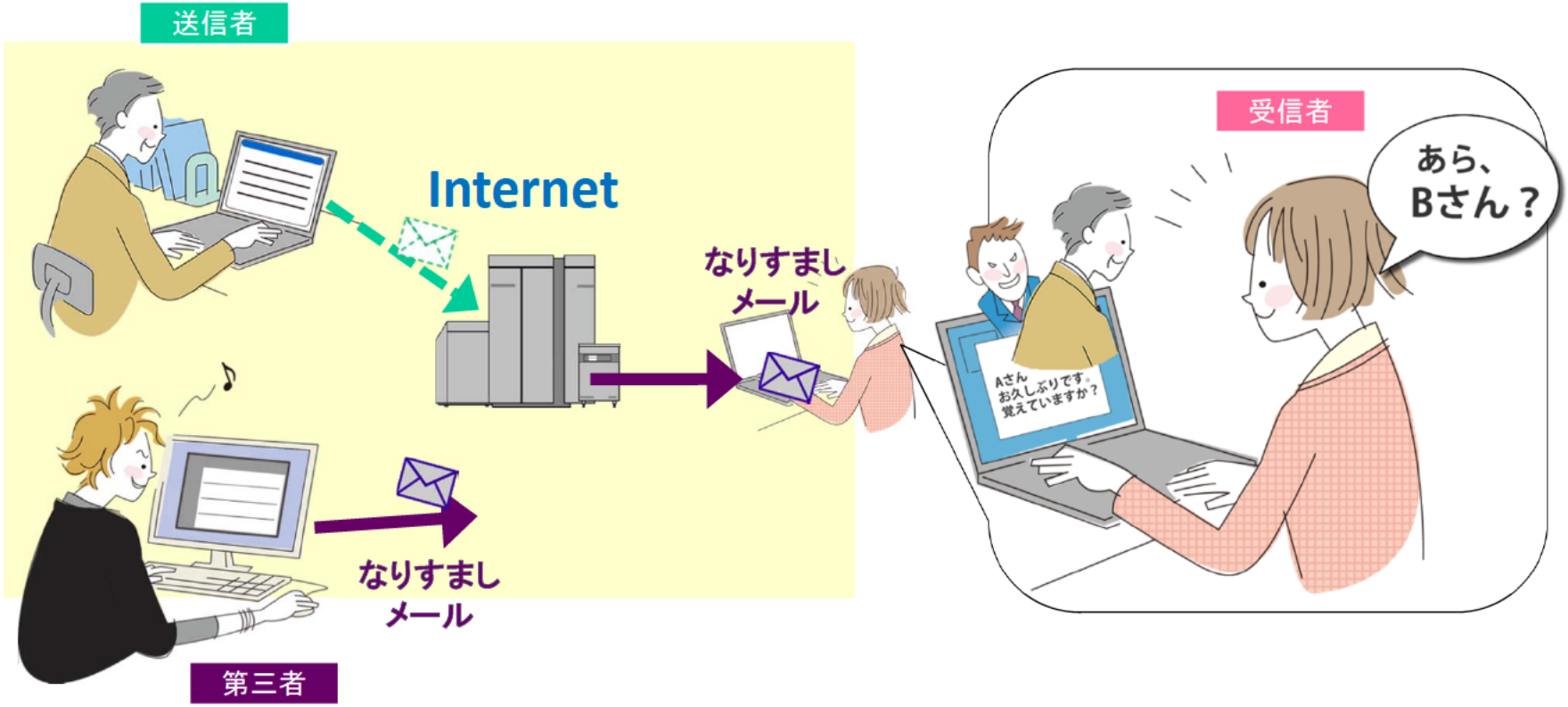
なりすましメールに気をつけよう

2012年　7月
迷惑メール対策推進協議会

自分自身のメールアドレスから、迷惑メールを送られてきて、驚いたことはありませんか?

メールの送信者情報「from: XXX@XXX」は、送信者が、簡単に書き換えることが可能です。
受信者のTom君のアドレスに書き換えたり、他人のアドレスに書き換えて、他人になりすますことも可能です。



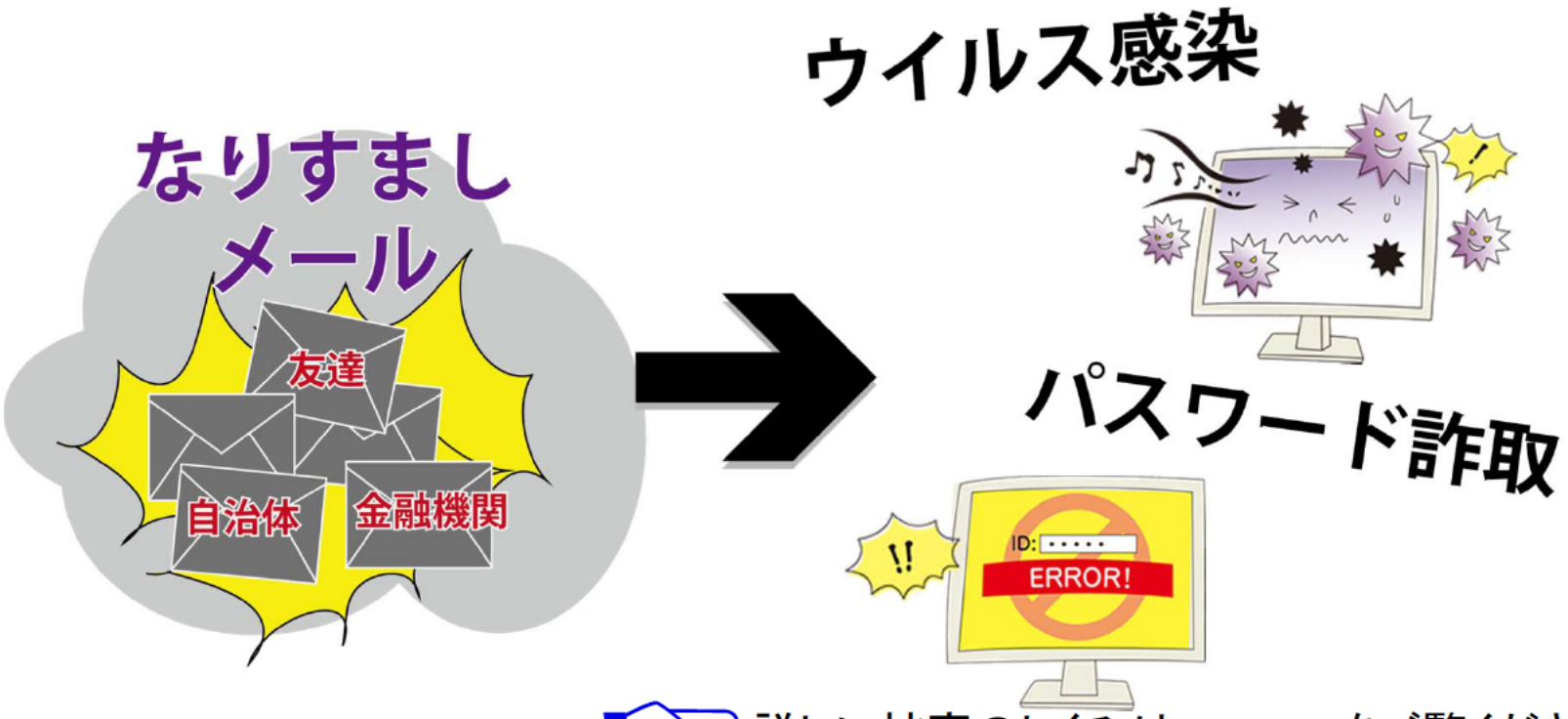
※ 送信者情報を偽ったなりすましメールの送信は、「特定電子メールの送信の適正化等に関する法律」（平成14年法律第26号）で禁止されている行為です。絶対してはいけません。

詳しい仕組みは、p13をご覧ください。

なりすましメールによって、様々な被害が発生しています。

◆金融機関になりすまして ⇒ 口座のパスワードの詐取
◆自治体になりすまして ⇒ ウイルスへの感染
◆受信者になりすまして ⇒ 出会い系サイトへの誘引

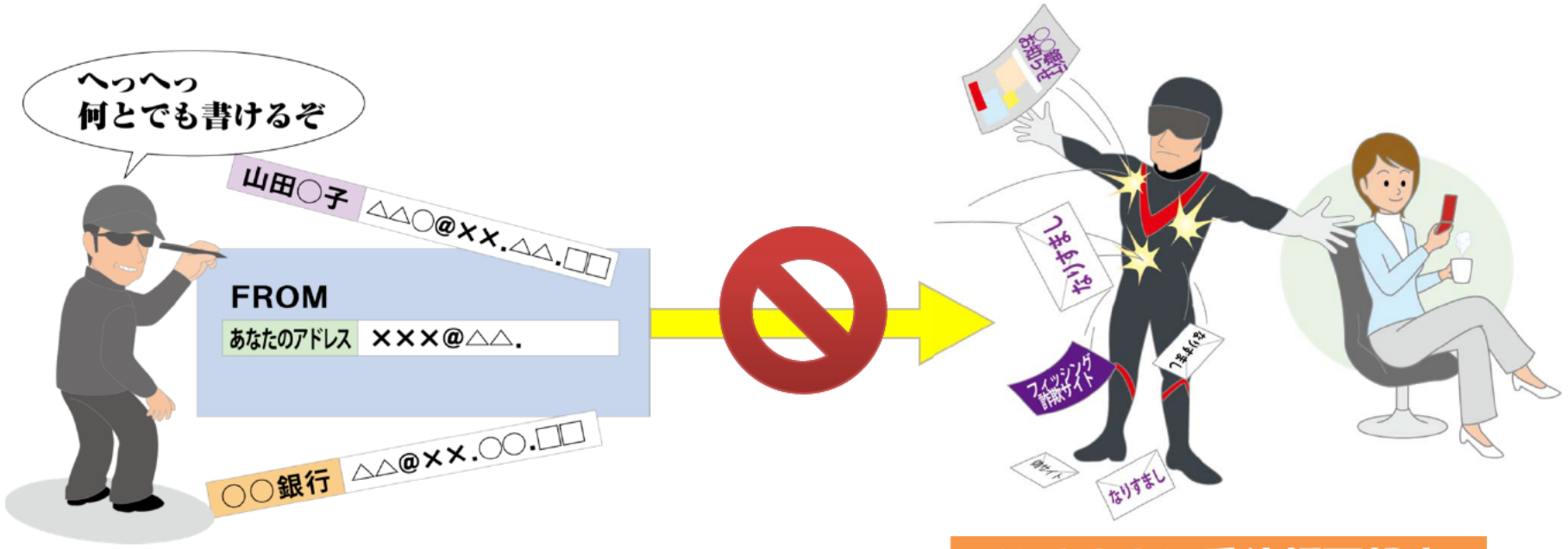
など



詳しい被害のしくみは、p14,15をご覧ください。

なりすましメールによって、金銭的損失など様々な被害を被るのは嫌ですね。では、どうすれば、なりすましメールにだまされないようにできるでしょうか?

インターネットサービスプロバイダや携帯電話会社では、なりすましメール対策サービスを提供しています。
こうしたサービスを活用し、なりすましメールを撃退しましょう。



詳しい仕組みは、p16をご覧ください。

インターネットサービスプロバイダや、携帯電話会社で提供している、なりすましメール対策サービスを利用することにより、次のような効果が期待できます！

■　送信者情報を偽って（なりすまされて）送信されたメールの受信をしないことが可能です！
（ISPでは、送信者情報を偽って送信されたメールを特定のフォルダに隔離したり、削除することも可能です）

■　フィッシング詐欺や標的型攻撃メールによる被害に巻き込まれるおそれが減少します！

※「なりすまし対策サービス」は、メール送信に使われた送信者情報等を元にしてメールの送信者を確認しているものですので、メールの内容まで信頼できるわけではありません。また、送信者が正規の送信者情報等を使用した上で、メールソフトに表示される送信者名を偽装した場合には対応が困難な場合があります。

参考

なお、なりすましメール対策サービスは、インターネットサービスプロバイダ、携帯電話会社や、ウェブメール等様々な方法で提供されています。

■ 携帯電話会社による迷惑メール対策サービスかんたん設定の中に組み込んでの提供

・この場合、かんたん設定を行えば、自動的になりすましメール対策サービスが利用できます。

■ インターネットサービスプロバイダ、携帯電話会社によるなりすましメール対策サービスの提供

・なりすましメール対策サービスの設定が必要です。

■ ウェブメール（Yahoo!メール等）でのなりすましメール対策サービスの提供

・なりすましメール対策サービスの設定が必要です。
・ウェブメールサービス提供者から送信されたメールであることが保証できる場合は、ブラウザのメール画面に信頼できるメールであることを示すアイコンを表示します（設定不要）

■ メールクライアントソフト（Outlook等)でのなりすましメール拒否機能の設定

・なりすましメール拒否機能の設定が必要です。

※ お使いになっているインターネットサービスプロバイダ、携帯電話会社、ウェブメール等によって、利用できる方法等が異なりますので、詳細はp17の方法によりご確認ください。

なりすましメール対策サービスの設定方法（例）

携帯電話（例：KDDI 1/2）

EZwebメールでは、迷惑メールでお困りのお客様向けに「auがオススメする設定」を提供しております。
設定頂くことで以下のメールフィルターが適用され、迷惑メールを削減することが可能です。

- 「なりすまし規制（高）」（送信ドメイン認証（Sender ID/SPF）技術を利用したメールの受信拒否）、
- 「迷惑メールおまかせ規制」（迷惑メールの疑いのあるメールを自動検知し規制する機能）
  （上記に加え、「拒否通知メール返信」を『返信する』に設定します。）

また、メール転送サービスを経由したメールやメーリングリストについては、なりすましメールの扱いとなりますが、
「指定リスト設定受信」で TO アドレス を指定することにより受信可能です

「auがオススメする設定」の設定方法※フィーチャーフォンの場合

①Eメール設定画面で「メールフィルタ」を選択します。
※機種によりメニューが異なる可能性がございます。

②迷惑メールフィルタ設定画面で「オススメの設定へ」を押下します。

③設定確認画面が表示されたら「登録」を選択します。登録完了画面が表示されたら、「迷惑メールおまかせ規制」「なりすまし規制（高）」の設定完了です。

「auがオススメする設定」の設定方法※スマートフォンの場合

①「その他設定」画面に遷移。
※機種によりメニューが異なる可能性がございます。

②迷惑メールフィルタ設定画面で「オススメの設定はこちら」を押下します。

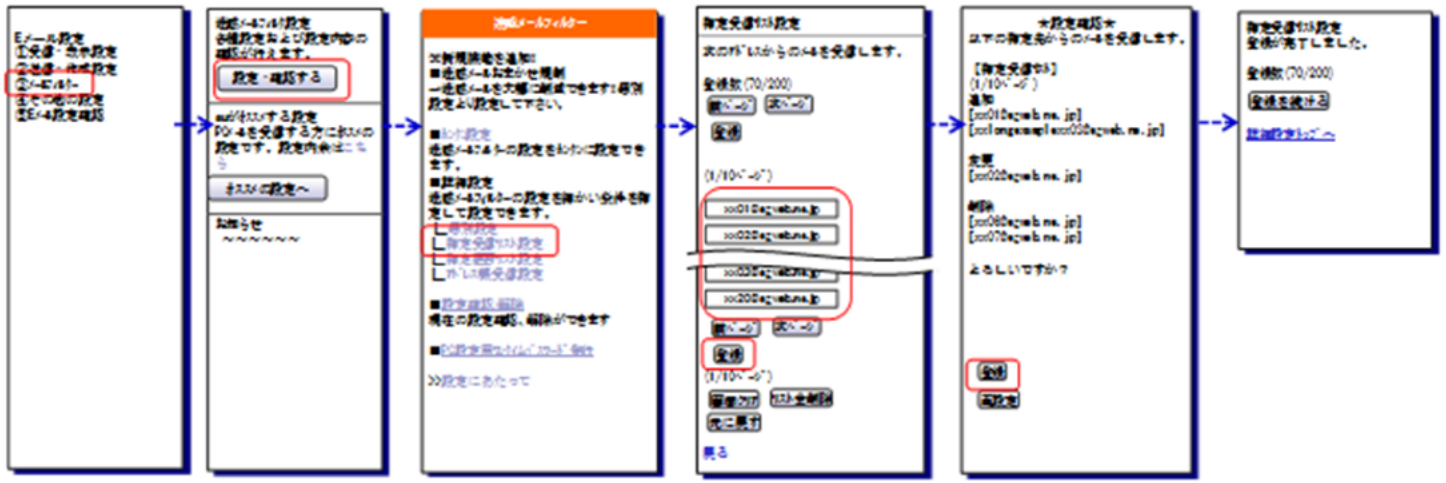
③設定確認画面が表示されたら「登録」を選択します。登録完了画面が表示されたら、「迷惑メールおまかせ規制」「なりすまし規制（高）」の設定完了です。

各社のサービスの確認方法は、p17をご覧ください。

なりすましメール対策サービスの設定方法（例）

携帯電話（例：KDDI 2/2）

「指定受信リスト設定」の設定方法※以下は、フィーチャーフォンの場合 です。（スマートフォンの場合、「Eメール設定」→「その他設定」→「迷惑メールフィルタ」からお入り下さい）



①Eメール設定画面で「メールフィルタを選択します。

※機種によりメニューが異なる可能性がございます。

②迷惑メールフィルタ設定画面で「設定・確認する」を押下します。

※次画面で、暗証番号（4桁）を入力ください。

③迷惑メールフィルタ設定画面で「指定受信リスト設定」を押下します。

④「指定受信リスト設定」のアドレス入力画面にて、受信許可したいアドレスを入力し、「登録」を押下します。

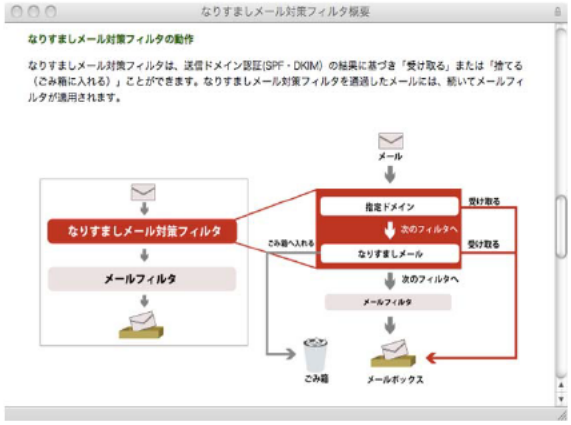
⑤設定確認画面が表示されたら、内容を確認し、「登録」を選択します。登録完了画面が表示されたら、「指定受信リスト設定」の設定完了です。

各社のサービスの確認方法は、p17をご覧ください。

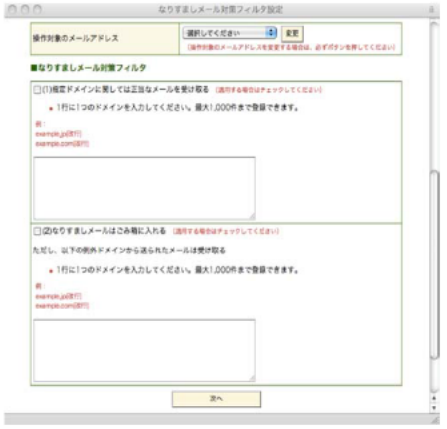
なりすましメール対策サービスの設定方法（例）

固定ＩＳＰ（例：IIJ）

IIJ4Uでは、送信ドメイン認証技術を用いた「なりすましメール対策フィルタ」が提供されており、フィルタ設定画面で、簡単に設定することが可能です。



なりすましメール対策フィルタで、なりすまされたメールをごみ箱にいれたり、指定されたドメインを優先的に受け取るなどの設定が行えます。



各社のサービスの確認方法は、p17をご覧ください。

なりすましメール対策サービスの設定方法（例）

ウェブメール（例：yahoo）

Yahoo!メールでは、送信ドメイン認証に「DKIM」「DomainKeys」「SPF」を採用しており、受信時のラベリングに加え、送信元詐称メールのフィルタリングにも活用していただけるよう、お客さま向けに設定画面を用意しています

■ **ラベリング**

受信時にDKIM, DomainKeys, SPFの認証結果をヘッダに格納します。メールソフトなどでフィルタリングする際に利用できます。

Received-SPF:	pass (web29xx.mail.yahoo.co.jp: domain of yahootaro@yahoo.co.jp designates 203.216.xxx.xxx as permitted sender) receiver=web29xx.mail.yahoo.co.jp; client-ip=203.216.xxx.xxx; envelope-from=yahootaro@yahoo.co.jp;
Authentication-Results:	mta1xx.mail.yahoo.co.jp from=yahoo.co.jp; **domainkeys=pass (ok)** ; **dkim=pass (ok)** header.i=@yahoo.co.jp

■ **Y! アイコン表示**

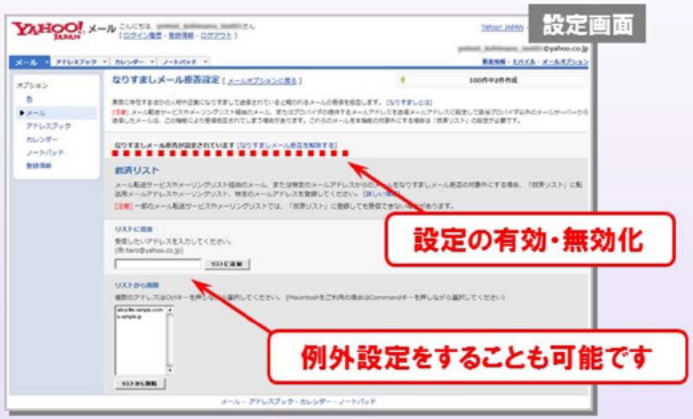
DomainKeys認証を利用し、Yahoo! JAPAN から送信されたメールであることが保証できる場合は、ブラウザのメール一覧画面に Y!アイコンを表示しています。フィッシングメールを簡単に見分けることが可能です。

画面例

■ **なりすまし受信拒否機能**

DomainKeys, SPFの認証結果により、送信元が詐称されている可能性がある場合は、メールを破棄し配送しない機能です。本機能を利用するには、お客様がご自分で設定を有効にする必要があります。

設定画面



（以上の情報は2012年5月現在のもので、今後仕様が変更されることもあります。）

各社のサービスの確認方法は、p17をご覧ください。

なりすましメール対策について（詳細）

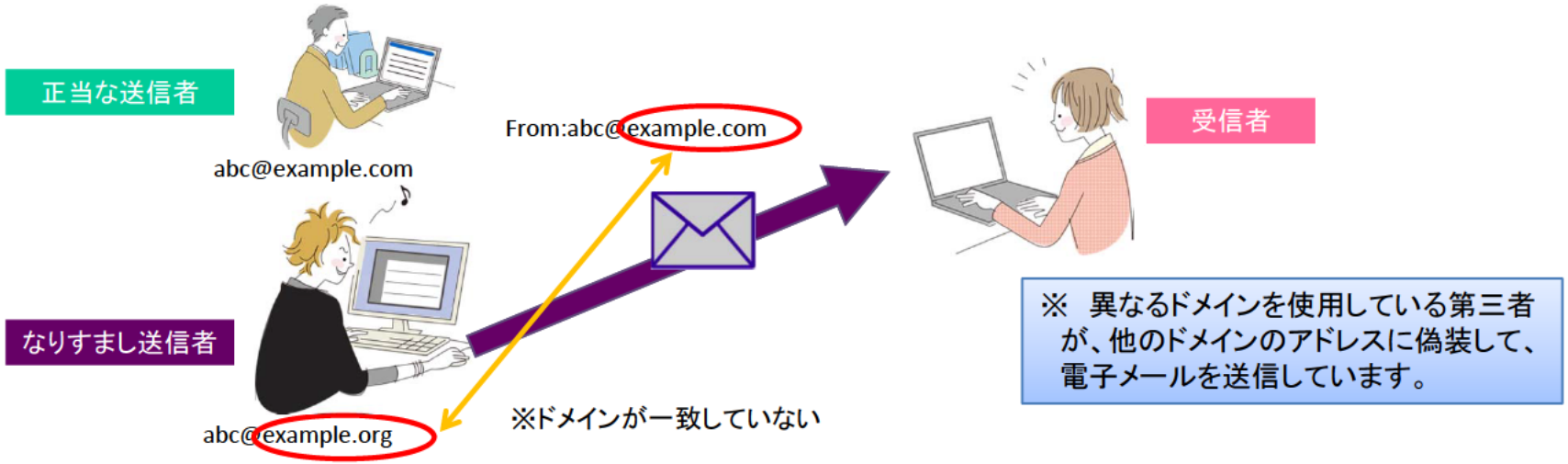
1．電子メールのなりすましについて①

電子メールの通信方式（プロトコル）であるSMTP（シンプル・メール・トランスファー・プロトコル）の標準規格は1970年代に策定されたものであり、送信者情報を確認する仕組みが備わっていません。
このため、電子メールは、送信者情報（Fromアドレス、ヘッダ情報等）について、いわゆる「なりすまし」が容易にできてしまい、近年では、様々な問題が発生しています。

(1) 電子メールの「なりすまし」とは

①「なりすまし」でない通常の電子メールの送信例

②「なりすまし」をしている電子メールの送信例



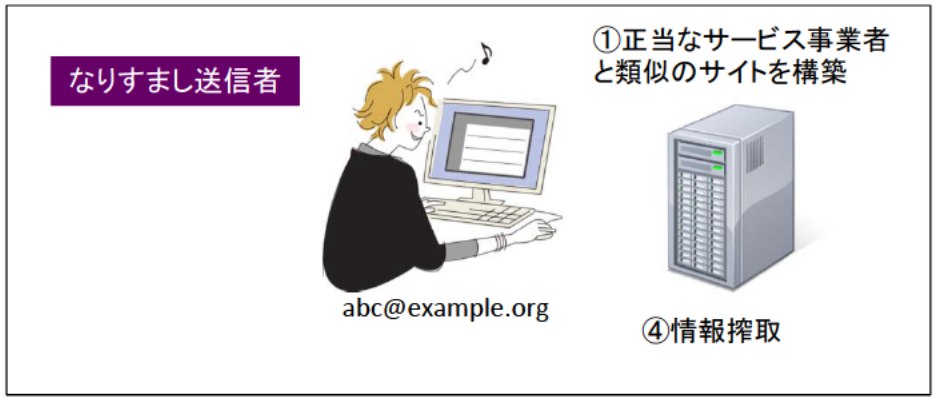
※　異なるドメインを使用している第三者が、他のドメインのアドレスに偽装して、電子メールを送信しています。

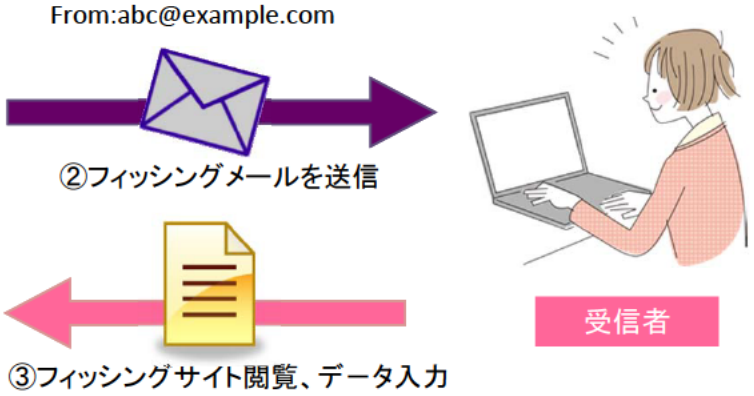
1．電子メールのなりすましについて②

(2) 電子メールの「なりすまし」による問題

①フィッシング詐欺に利用される

正当なサービス事業者になりすまし、フィッシングサイトをリンク先としたURLを文面に含めたフィッシングメールを送信し、フィッシングサイトにアクセスさせて、受信者の個人情報、ID、パスワード等を搾取しようとします。



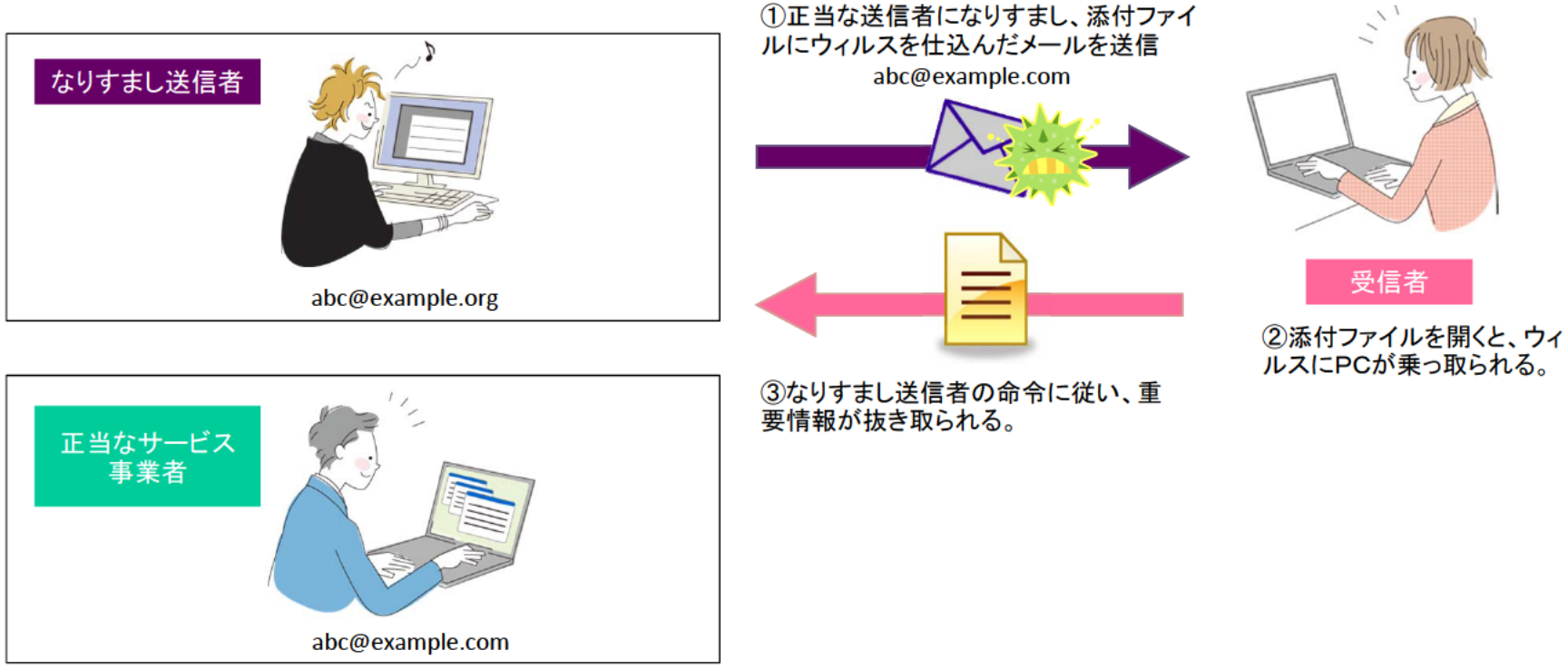


1．電子メールのなりすましについて③

(2) 電子メールの「なりすまし」による問題

②知り合い等になりすまされ、コンピュータウィルスに感染させられる

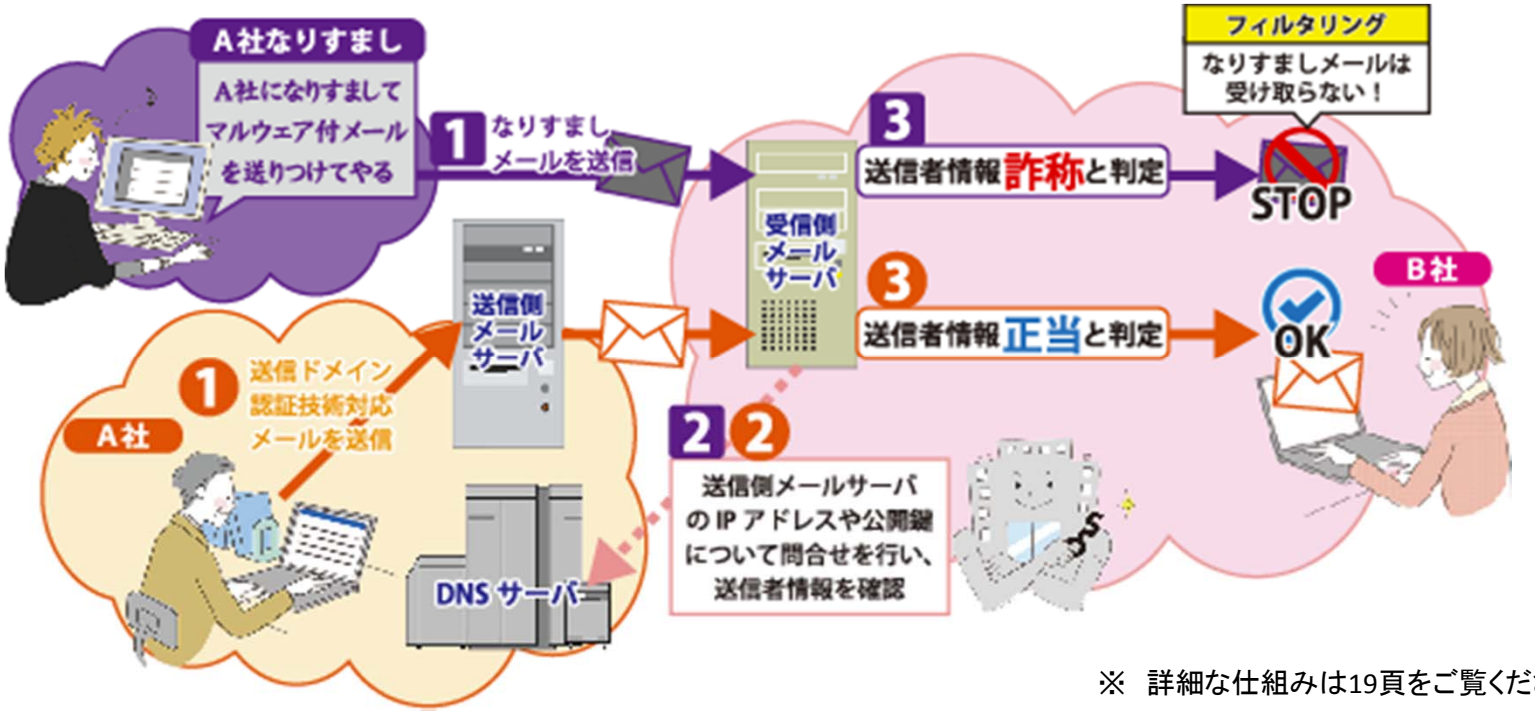
正当な送信者になりすますとともに、タイトル、本文等に巧妙な記述をすることによって、添付ファイルを開かせたり、電子メール本文に記載されたURLをクリックさせて、コンピュータウィルスに感染させようとします。



2．電子メールのなりすましを防止するための技術（送信ドメイン認証技術）

■　電子メールのなりすましを防止するため、インターネットの標準規格として、「送信ドメイン認証技術」という技術があります。
■　インターネットサービスプロバイダーや携帯電話事業者では、「送信ドメイン認証技術」を活用して、なりすましメール対策サービスを提供しています。
■　「送信ドメイン認証技術」を活用したサービスを利用することで、利用者は電子メールをより安心して利用することができます！

送信ドメイン認証技術の概要



※　詳細な仕組みは19頁をご覧ください。

3．送信ドメイン認証技術を活用したサービスの確認方法

ご利用の携帯電話事業者、ＩＳＰ等が送信ドメイン認証技術を活用したサービスを提供しているか次の手順で、ご確認ください。

1　お使いの携帯電話事業者、ＩＳＰ等の確認

まず、お使いの携帯電話事業者、ＩＳＰ等がどこなのかを確認します。

2　お使いの携帯電話事業者、ＩＳＰ等の対応状況の確認

次に、お使いの携帯電話事業者、ＩＳＰ等が、送信ドメイン認証技術に対応したサービスを提供しているかどうかを確認しましょう。

送信ドメイン認証技術を活用したサービスを提供している場合

※　日本データ通信協会迷惑メール相談センターのウェブページで、次ページのように、携帯電話事業者やISPの対応状況を一覧にして公表しています。(http://www.dekyo.or.jp/soudan/auth/)

※　上記の情報は年2回の調査によるものですので、確実な情報は、各携帯電話事業者、ISPにご確認下さい。

3　送信ドメイン認証技術を活用したサービスの利用方法の確認

送信ドメイン認証技術を活用したサービスの利用方法は、携帯電話事業者、ＩＳＰ等により異なりますので、お使いの携帯電話事業者、ＩＳＰ等にご確認いただき、ご利用下さい。

4. 送信ドメイン認証技術の利用に際しての留意点

送信ドメイン認証技術の利用にあたっては、以下のような点に留意が必要です！

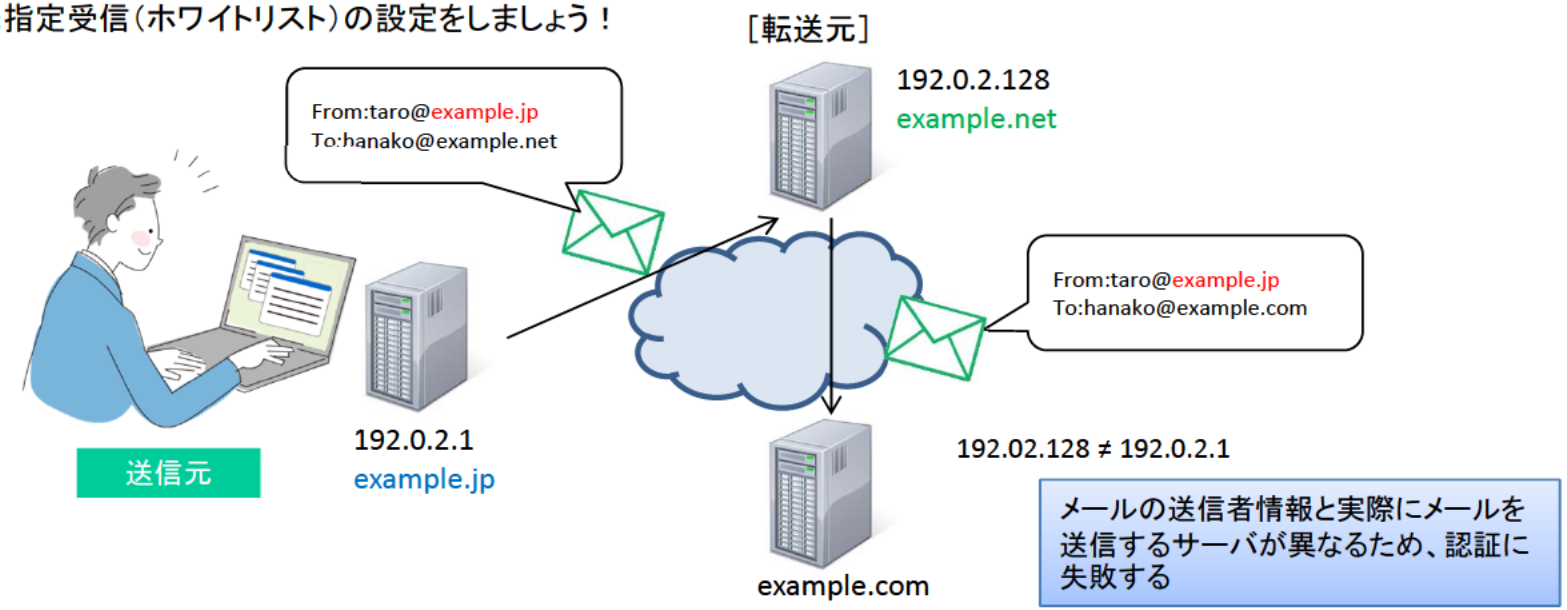
送信者が認証されたメールでも、内容まで信頼できる訳ではありません

・ 送信ドメイン認証技術で認証された電子メールは、あくまでも、正規の送信元ドメインから送信されたことが確認されているだけですので、その内容まで信頼できる訳ではありません。例えば、出会い系サイト事業者が送信ドメイン認証技術に対応して、自身のサイトに誘導する広告宣伝メールを送信してくる場合もあります。

メールを転送している場合には、SPF認証が失敗することがあります

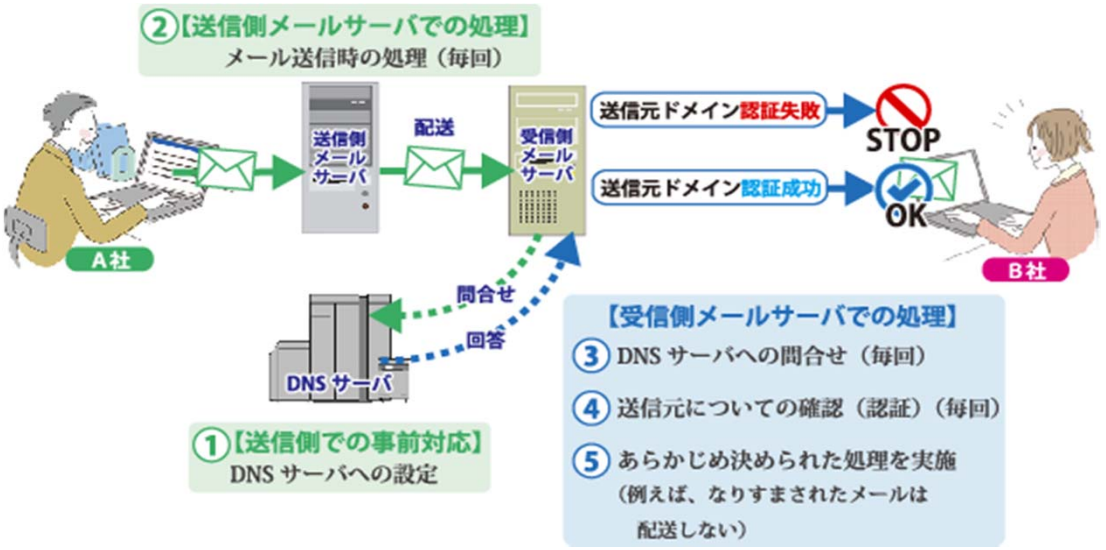
・ 送信ドメイン認証技術のうち、SPFという技術を利用している場合、メールを転送していると、なりすましていないメールでも、認証に失敗することがあります。これは、メールの転送時に、送信元の送信者情報をそのままにして、転送してしまうことが原因です。

・ 宛先指定受信（ホワイトリスト）の設定をしましょう！



（参考1）送信ドメイン認証技術の詳細

■　送信ドメイン認証技術には、SPF/Sender ID方式とDKIM方式とがあり、それぞれ認証の方式が若干異なります（実際の処理はもっと複雑ですが、模式化して簡単にしています）



	ネットワーク方式の送信ドメイン認証技術 SPF / Sender ID		電子署名方式の送信ドメイン認証技術 DKIM
①	送信側のメールサーバで、ＤＮＳサーバに、自らのドメインのメールが送信されるメールサーバのＩＰアドレス等の情報を記述	①	送信側のメールサーバで、認証に用いる公開鍵暗号技術による鍵ペア（公開鍵・暗号鍵）を生成し、公開鍵をＤＮＳサーバで公開
②	（個別のメールの送信にあたっては、特別の処理なし）	②	個別のメールの送信にあたり、メールの内容（ヘッダ・本文）の情報を用い、①の暗号鍵により電子署名を作成し、メールに添付
③	受信側のメールサーバでは、メールを受信した際に、送信者のメールアドレスのドメインのＤＮＳサーバに、送信側メールサーバについて問合せ（取得）	③	受信側のメールサーバでは、メールを受信した際に、送信者のメールアドレスのドメインのＤＮＳサーバに、当該ドメインの公開鍵を問合せ（取得）
④	メール受信の際に通信した相手方のメールサーバのＩＰアドレスが、③で取得したＩＰアドレスと一致しているかどうか確認（一致していれば認証成功）	④	受信したメールの電子署名を③で取得した公開鍵で検証し、受信したメールの内容と一致するかどうか確認（一致していれば認証成功）

（参考2）一般財団法人日本データ通信協会迷惑メール相談センターにおける携帯電話事業者・ＩＳＰ等の送信ドメイン認証技術を活用したサービス対応状況一覧

一般財団法人日本データ通信協会迷惑メール相談センターでは、携帯電話事業者・ＩＳＰ等の送信ドメイン認証技術を活用したサービスの対応状況一覧を公表しています。
（http://www.dekyo.or.jp/soudan/auth/）

携帯・PHS事業者の対応状況の例

No.	事業者	サービス名※1	送信※2		受信※3				詳細
			SPF/ SenderID	DKIM/ domainKeys	SPF/ SenderID		DKIM/ domainKeys		
					ラベリング	フィルタリング	ラベリング	フィルタリング	
1	イー・アクセス株式会社	EMnetメール	☆	—	◎	☆	—	—	
2	株式会社ウィルコム	WILLCOM（Eメール）	☆	—	—	—	—	—	
3	株式会社NTTドコモ	docomo（iモード）	☆	—	◎	☆	—	—	送信/受信
4	株式会社NTTドコモ	spモード	☆	—	—	☆	—	—	
5	KDDI株式会社	au(EZweb)	☆	—	◎	☆	—	—	
6	ソフトバンクモバイル株式会社	SoftBank（S!メール）	☆	—	—	—	—	—	—

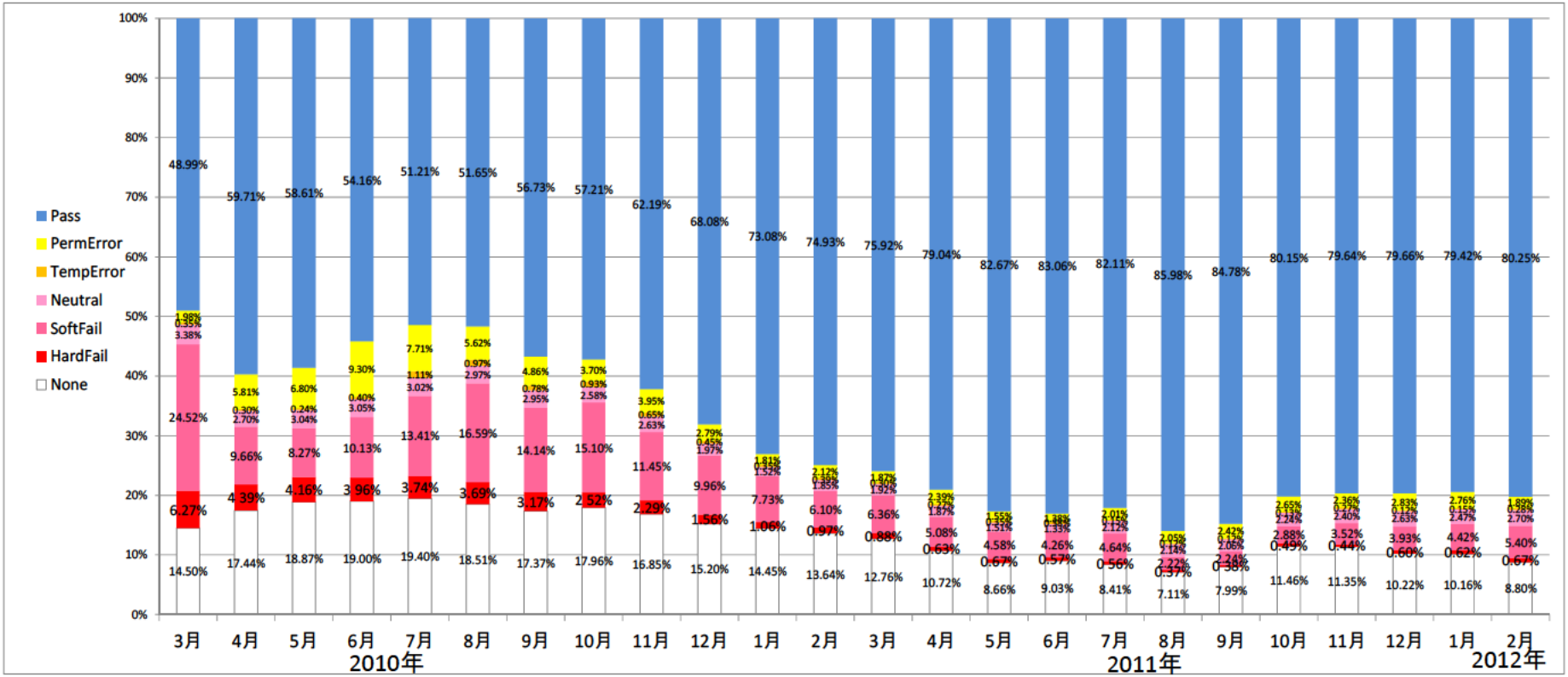
ISPの対応状況の例

No.	事業者	サービス名※1	SPF/ SenderID	DKIM/ domainKeys	SPF/ SenderID		DKIM/ domainKeys		詳細
					ラベリング	フィルタリング	ラベリング	フィルタリング	
1	株式会社アイエフネット	アイエフネットインターネットサービス	☆	—	○	—	—	—	—
2	株式会社アイエフネット	IP ONE インターネットサービス	☆	—	○	—	—	—	—
3	イッツ・コミュニケーションズ株式会社	イッツコム かっとびインターネット	☆	—	○	—	◎	—	—
4	株式会社インターネットイニシアティブ	IIJ 4U	☆	☆	◎	☆	◎	☆	
5	株式会社インターネットイニシアティブ	IIJ mio	☆	☆	◎	☆	◎	☆	
6	株式会社STNet	Pikara	☆	—	—	—	—	—	—
7	株式会社STNet	STCN	☆	—	○	—	—	—	—
8	株式会社STNet	Netwave	☆	—	—	—	—	—	—
9	株式会社NTT-ME	WAKWAK	☆	—	—	—	—	—	—
10	ＮＥＣビッグローブ株式会社	BIGLOBE	☆ (2005/11)	—	◎ (2006/09)	—	◎ (2007/09)	—	

（参考3）送信ドメイン認証技術の普及状況（流量ベース①）

日本で実際に流通しているメールにおける送信ドメイン認証技術の対応状況を見ますと、約９割のメールがネットワーク方式であるSPF/Sender IDに対応しています。
また、電子署名方式であるDKIMは、約２割のメールが対応しています。

■ 実際に流通している電子メールにおけるSPF／Sender IDの対応状況



（参考3）送信ドメイン認証技術の普及状況（流量ベース②）

■ 実際に流通している電子メールにおけるDKIMの対応状況